

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION**

**JULIO VARGAS, individually and on behalf
of all others similarly situated,**

Plaintiff,

v.

**VENTURE TRANSPORTATION
PARTNERS, LLC d/b/a VENTURE
LOGISTICS**

Defendant

Case No.

CLASS ACTION COMPLAINT

Plaintiff, Julio Vargas, individually and on behalf of all others similarly situated, brings this action against Defendant, Venture Transportation Partners, LLC d/b/a Venture Logistics (“Defendant” or “Venture”), and alleges as follows:

NATURE OF THE ACTION

1. In May 2023, Venture, a national full-service logistics company, lost control over its employees’ highly sensitive personal information in a data breach by cybercriminals (the “Data Breach”).

2. On or about August 18, 2023, Venture sent notice to its current and former employees to notify them of “a recent incident experienced by [Venture] and its affiliates that may impact the privacy of certain information.”¹

¹ See **Exhibit A**, Sample Data Breach Notice Letter (the “Notice Letter”), available at <https://apps.web.maine.gov/online/aeviewer/ME/40/8734fdbd-840b-4249-b05b-748affc1d8cb.shtml> (last accessed Jun. 5, 2024).

3. Specifically, on May 13, 2023, “[Venture] discovered unusual activity on [its] network.” Venture discovered through an investigation that “an unknown party acquired certain information on parts of [its] network.” *Id.*

4. As a result of the Data Breach, Venture reported that certain Personally Identifying Information² and Protected Health Information³ (collectively “PII”) of Venture’s current and former employees was affected.

5. This compromised PII included current and former employees’ names, dates of birth, Social Security numbers, driver’s license/state issued identification numbers, financial account information, credit/debit card information, medical information, and health insurance information. Ex. A.

6. Upon information and belief, victims of the Data Breach did not start receiving letters notifying them of the Data Breach or detailing which specific types of their PII was compromised until over three months after Venture discovered the Data Breach. *See* Ex. A.

² The Federal Trade Commission defines “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” 17 C.F.R. § 248.201(b)(8). To be clear, according to Venture, not every type of information included in that definition was compromised in the breach.

³ Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations (“HIPAA”), “protected health information” is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. A “covered entity” is further defined as, *inter alia*, a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA. *Id.* *Covered entity*. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP’T FOR HEALTH & HUM. SERVS., <https://bit.ly/30Bg7gZ> (last accessed Nov. 18, 2021). Venture is clearly a “covered entity” and some of the data compromised in the Data Breach that this action arises out of is “protected health information”, subject to HIPAA.

7. The Notice Letter urged Plaintiff and victims of the Data Breach to “remain vigilant against incidents of identity theft and fraud,” and to review account statements and monitor credit reports for suspicious or unauthorized activity. *Id.*

8. The Notice Letter also encouraged Plaintiff and other victims of the Data Breach to consider, *inter alia*, placing credit freezes on their credit files, place or extend fraud alerts on their credit file, monitoring accounts, ordering copies of their credit reports, and reviewing statements received from health insurance and health care providers. *Id.*

9. Venture offered 12 or 24 months of complimentary credit monitoring through IDX to the affected victims as a result of the Data Breach.

10. As a consequence of the Data Breach, Plaintiff and Class members’ sensitive PII has been released into the public domain and they have had to, and will continue to have to, spend time to protect themselves from fraud and identity theft.

11. Plaintiff and members of the proposed Class are victims of Venture’s negligence and failure to honor its promise to keep PII private. Specifically, Plaintiff and members of the proposed Class trusted Venture with their PII. But Venture betrayed that trust. Venture failed to properly use up-to-date security practices to prevent the Data Breach, and when the Data Breach was discovered, Defendant failed to promptly notify victims of the Data Breach of the types of information that was stolen.

12. Venture’s negligence and failure to abide by its promise to maintain the privacy of its employees’ PII caused real and substantial damage to Plaintiff and members of the proposed Class.

13. Further, because this same information remains stored in Venture’ systems, Plaintiff and Class members have an interest in ensuring that Venture takes the appropriate

measures to protect their PII against future unauthorized disclosures.

14. Plaintiff, individually and on behalf of all others similarly situated, thus brings this class action against Venture for failing to adequately secure and safeguard the PII of Plaintiff and the Class, breaching the terms of Venture's implied contracts with its patients, and failing to comply with industry standards regarding the use and transmission of PII.

15. Plaintiff is a former Venture employee and Data Breach victim, who entrusted his PII to Defendant. Plaintiff brings this class action on behalf of all employees harmed by Venture's misconduct.

PARTIES

16. Plaintiff Julio Vargas is a resident and citizen of Florida. He is a former employee of Defendant Venture and worked there from approximately March 2021 to July 2022. As a condition of Plaintiff Vargas's employment at Venture, he was required to provide his PII to Defendant.

17. Plaintiff Vargas received the Notice Letter directly from Defendant Venture, via U.S. mail, dated August 18, 2023. If Mr. Vargas had known that Defendant would not adequately protect his PII, he would not have entrusted Defendant with his PII or allowed Defendant to maintain this sensitive PII.

18. Defendant, Venture, is an Indiana corporation with its principal place of business in Carmel, Indiana. Its headquarters are located at 1101 Harding Court, Indianapolis, Indiana 46217.

JURISDICTION & VENUE

19. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of \$5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and

minimal diversity exists because many putative class members including Plaintiff are citizens of a different state than Defendants. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

20. This Court has personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business in Indiana and committed tortious acts in Indiana.

21. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this district.

BACKGROUND FACTS

A. Venture

22. Venture is the “one of the nation’s largest full-service logistics companies.”⁴ “For over 25 years, Venture has served as a full-service logistics partner in North America and across the globe, offering a vast array of specialized services to get the job done safely, successfully, and on time -24/7, 365.”⁵

23. To work at Venture, Venture requires its employees to disclose their PII.

24. That PII includes their names, dates of birth, Social Security numbers, driver’s license/state issued identification numbers, financial account information, credit/debit card information, medical information, and health insurance information.

25. In exchange, Venture implicitly promises to secure its employees’ PII.

26. But, on information and belief, Venture never implemented or enforced the reasonable cybersecurity measures and policies necessary to deliver on those promises.

B. Venture fails to safeguard employee PII

⁴ <https://www.venturelogistics.com/about/> (last acc. Jun. 5, 2024).

⁵ *Id.*

27. Plaintiff is a former Venture employee. Plaintiff was employed with Venture from March 2021 to July 2022.

28. Venture collects and maintains employee PII in its computer systems as a condition of their employment.

29. In collecting and maintaining the PII, Venture implicitly promised it would safeguard the data according to state and federal law and its internal policies.

30. Despite those promises, Venture lost control over its employees' PII.

31. In May 2023, hackers bypassed Venture's cybersecurity undetected and accessed its employees' PII.

32. Venture detected the breach on May 13, 2023. Venture concluded its investigation of the Data Breach on June 19, 2023. Venture's investigation revealed that "an unknown party acquired certain information on parts of [Venture's] network." Ex. A.

33. Thus, cybercriminals accessed and stole employees' PII, including their names, dates of birth, Social Security numbers, driver's license/state issued identification numbers, financial account information, credit/debit card information, medical information, and health insurance information.

34. Venture did not notify its employees that hackers had stolen their information, nor would it until August 2023.

35. By June 19, 2023, Venture concluded its "investigation." However, Venture did not notify its employees about the breach until two months later, on August 18, 2023.

36. Venture is warning its employees to monitor their credit scores and enroll in credit monitoring, thus recognizing that employees should protect themselves from identity theft following the Data Breach.

37. On information and belief, Venture failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over employee PII. Venture's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII. Further, the Breach Notice makes clear that Venture cannot, or will not, determine the full scope of the Data Breach, as it has been unable to determine exactly what information was stolen and when.

C. Plaintiff's Experience

38. Plaintiff is a former Venture employee, having been employed with Venture from March 2021 to July 2022.

39. As a condition of Plaintiff's employment, Venture required Plaintiff to disclose his PII.

40. Plaintiff provided his PII to Venture and trusted that the company would use reasonable measures to protect it according to Venture's internal policies and state and federal law.

41. Plaintiff Vargas is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

42. At the time of the Data Breach—May 13, 2023—Defendant retained Plaintiff's PII in its system, despite no longer maintaining an employment relationship with Plaintiff.

43. Plaintiff Vargas received the Notice Letter, by U.S. mail, directly from Defendant, dated August 18, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his full name, address, Social Security number, driver's license/state issued identification number, financial account information, credit/debit card information, medical information, and health insurance information. Plaintiff has spent significant time remedying the breach—time dealing with the Data Breach, valuable time

Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

44. Upon receiving the Notice Letter from Defendant, Plaintiff Vargas has spent significant time dealing with the consequences of the Data Breach including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, signing up for the credit monitoring and identity theft insurance offered by Defendant, and contacting financial institutions to ensure his accounts are secure.

45. Subsequent to the Data Breach, Plaintiff Vargas has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

46. Plaintiff Vargas additionally suffered actual injury and damages as a result of the Data Breach. Implied in his employment contract with Defendant was the requirement that it adequately safeguard his PII and that it would delete or destroy his PII after Defendants were no longer required to retain it. Plaintiff Vargas would not have worked for Defendant had Defendant disclosed that it lacked data security practices adequate to safeguard PII.

47. Plaintiff Vargas further suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant

for the purpose of employment, which was compromised by the Data Breach.

48. Plaintiff Vargas also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number, being in the hands of criminals.

49. Plaintiff Vargas has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII being placed in the hands of unauthorized third parties and possibly criminals.

50. Plaintiff Vargas has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

D. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

51. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

52. As a result of Venture's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their PII is used;
- b. The diminution in value of their PII;
- c. The compromise and continuing publication of their PII;
- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent,

detect, contest, and recover from identity theft and fraud;

- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen PII; and
- h. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

53. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to \$1,000.00 depending on the type of information obtained.

54. The value of Plaintiff and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

55. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

56. One such example of criminals using PII for profit is the development of "Fullz" packages.

57. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

58. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email

addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

59. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

60. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

E. Defendant failed to adhere to FTC guidelines.

61. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

62. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide

for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

- a. protect the personal customer information that they keep;
- b. properly dispose of personal information that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network's vulnerabilities; and
- e. implement policies to correct security problems.

63. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

64. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

65. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

66. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

67. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

68. Plaintiff brings this nationwide class action on behalf of himself and all other persons similarly situated (“the Class”) pursuant to Rule 23(a) of the Federal Rules of Civil Procedure, and Fed. R. Civ. P. 23(b)(3).

69. Plaintiff proposes the following Class definition (the “Class”), subject to amendment based on information obtained through discovery:

All persons residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the Data Breach reported by Defendant in August 2023, including all persons who received the Notice Letter.

70. Excluded from the Classes are Defendant’s officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

71. Plaintiff reserves the right to amend the definition of the Class or add a class or subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

72. Certification of Plaintiff’s claims for class-wide treatment is appropriate because Plaintiff can prove the elements of Class Members’ claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

73. This action satisfies the requirements for a class action under Fed. R. Civ. P. 23(a)(1)-(3) and Fed. R. Civ. P. 23(b)(2), including requirements of numerosity, commonality,

typicality, adequacy, predominance, and superiority.

74. **Numerosity, Fed. R. Civ. P. 23(a)(1):** The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the PII of approximately 9,339 current and former employees of Defendant was compromised in the Data Breach. Such information is readily ascertainable from Defendant's records.

75. **Commonality, Fed. R. Civ. P. 23(a)(2):** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, the FTC Act;
- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether computer hackers obtained Class Members' PII in the Data Breach;
- f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- g. Whether Plaintiff and the Class Members suffered legally cognizable damages as

a result of Defendant's misconduct;

- h. Whether Defendant breached the covenant of good faith and fair dealing implied in its contracts with Plaintiff and Class Members;
- i. Whether Defendant's acts violated Indiana law, and;
- j. Whether Plaintiff and the Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

76. **Typicality, Fed. R. Civ. P. 23(a)(3):** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same violations of law. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

77. **Adequacy, Fed. R. Civ. P. 23(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

78. **Predominance, Fed. R. Civ. P. 23(b)(3):** Defendant have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data—PII—was stored on the same computer systems and unlawfully exposed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

79. **Superiority, Fed. R. Civ. P. 23(b)(3):** A class action is a superior method for the fair and efficient adjudication of this controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, and joinder of

the Class Members is otherwise impracticable. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

- a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.
- b. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.
- c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendant.
- d. This lawsuit presents no difficulties that would impede its management by the

Court as a class action. The class certification issues can be easily determined because the Class includes only Venture's employees, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendant's records, such that direct notice to the Class Members would be appropriate.

80. In addition, Defendant have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

81. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant failed to timely and adequately notify the public of the Data Breach;
- b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

- f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

82. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

**COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)**

83. Plaintiff realleges all previous paragraphs as if fully set forth below.

84. Plaintiff and members of the Class entrusted their PII to Defendant. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII in their care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

85. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in their employ who were responsible for making that happen.

86. Defendant owed to Plaintiff and members of the Class a duty to notify them within

a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

87. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and members of the Class's personal information and PII.

88. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

89. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Class's and the importance of exercising reasonable care in handling it.

90. Defendant breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff and members of the Class's injury. Defendant further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from

the Data Breach and Plaintiff and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

91. Defendant's breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

92. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

93. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

94. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive PII.

95. Defendant violated their duty under Section 5 of the FTC Act by failing to use

reasonable measures to protect their employees' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to their employees in the event of a breach, which ultimately came to pass.

96. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

97. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PII.

98. Defendant breached their respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

99. Defendant's violation of Section 5 of the FTC Act and their failure to comply with applicable laws and regulations constitutes negligence per se.

100. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

101. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet their duties and that their breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

102. Had Plaintiff and members of the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

103. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

**COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)**

104. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

105. Defendant offered to employ Plaintiff and members of the Class in exchange for their PII.

106. In turn, Defendant agreed it would not disclose the PII it collects to unauthorized persons. Defendant also promised to safeguard employee PII.

107. Plaintiff and the members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for employment with Defendant.

108. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

109. Plaintiff and the members of the Class would not have entrusted their PII to

Defendant in the absence of such agreement with Defendant.

110. Defendant materially breached the contract(s) it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into their computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and members of the Class by:

- a. Failing to properly safeguard and protect Plaintiff and members of the Class's PII;
- b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and
- c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

111. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of their agreement(s).

112. Plaintiff and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

113. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to their form.

114. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of

inaction, and fair dealing may require more than honesty.

115. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

116. In these and other ways, Defendant violated its duty of good faith and fair dealing.

117. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

**COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)**

118. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

119. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

120. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of services through employment.

121. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class. Defendant also benefited from the receipt of Plaintiff and members of the Class's PII, as this was used to facilitate their employment.

122. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Class's services and their PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII or worked for Defendant at the payrates they did had they known Defendant would not adequately protect their PII.

123. Defendant should be compelled to disgorge into a common fund for the benefit of

Plaintiff and members of the Class all unlawful or inequitable proceeds received by it because of their misconduct and Data Breach.

**COUNT V
BAILMENT
(On Behalf of Plaintiff and the Class)**

124. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

125. Plaintiff, the Class Members, and Defendant contemplated a mutual benefit bailment when the Plaintiff and putative members of the Class transmitted their PII to Defendant solely for the purpose of obtaining employment.

126. Plaintiff and the Class entrusted their PII to Defendant for a specific purpose—to obtain employment—with an implied contract that the trust was to be faithfully executed, and the PII was to be accounted for when the special purpose was accomplished.

127. Defendant accepted the Plaintiff's and the Class's PII for the specific purpose of employment.

128. Defendant was duty bound under the law to exercise ordinary care and diligence in safeguarding Plaintiff's and the Class's PII.

129. Plaintiff's and the Class's PII was used for a different purpose than the Plaintiff and the Class intended, for a longer time period and/or in a different manner or place than Plaintiff and the Class intended.

130. As set forth in the preceding paragraphs, Plaintiff and the Class Members were damaged thereby.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

- A. Certifying this case as a class action on behalf of Plaintiff and the proposed Classes, appointing Plaintiff as class representative, and appointing their counsel to represent the Classes;
- B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;
- C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;
- D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;
- E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- G. Awarding attorneys' fees and costs, as allowed by law;
- H. Awarding prejudgment and post-judgment interest, as provided by law;
- I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and
- J. Granting such other or further relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff hereby demand a trial by jury on all issues so triable.

Dated: June 6, 2024

Respectfully submitted,

s/ Lynn A. Toops
Lynn A. Toops (No. 26386-49)
Amina A. Thomas (No. 34451-49)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400

Indianapolis, IN 46204
T: (317) 636-6481
F: (317) 636-2593
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

J. Gerard Stranch, IV *
Andrew E. Mize*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel J. Strauss*
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

**Pro Hac Vice Application Forthcoming*

Counsel for Plaintiff and the Proposed Class